NIAC Vulnerability Disclosure Working Group (VDWG)

Status Report
National Infrastructure Advisory Council
October 14, 2003

John Thompson
Symantec

John Chambers
Cisco Systems

Tasks

- Develop global guidelines for handling security vulnerabilities from initial report to final resolution
- Derive specific policy recommendations for the President

Participants

- Working Group Co-Chairs:
  - John Chambers, Cisco Systems
  - John Thompson, Symantec
- Working Group members: ISS (IT-ISAC), Mitre, CERT/CC, Verizon (Telecom-ISAC), Counterpane, Fannie Mae (FS-ISAC), UC Davis, Microsoft (OIS), ISC, DHS/IAIP
- Additional feedback and input from FIRST, NANOG, USENIX

Reviewer Comments

- Consistent vulnerability scoring methodology will be a key outcome
  - Current methods do not agree—disagreements on threat severity affect handling
  - Consistent scoring would support predictable threat management choices
  - Very difficult problem, but necessary to solve
- Communications section comprehensive and clear
  - Covers discoverers, vendors, coordinators, governments, users
  - Desired redundancy must be balanced by reality
  - Encryption differences must be resolved
- Reviewers endorse global scope and public-private partnership emphasis

Task Complexity Requires Time to Complete

- Real challenge: balancing desire to disclose with need to protect
  - Developing decision support process
  - Process must include predictability, consequences, wide acceptance, and dependability
  - Meat of the report—most difficult to complete
  - January 2004 delivery
- Recommend NIAC commission scoring research task to provide common perspective
  - Reinstate scoring subgroup of this WG
  - Conduct research concurrent with this report development—(6-month project)
  - Develop common scoring methodology
  - Report separately, but will support overall framework

Next Steps

- Revised schedule:
  - 07/14: First draft reviewed by working group
  - 08/13: External reviewers solicited
  - 08/22: 1st round of external comments received
  - 08/25-09/12: Additional comments and discussion
  - 10/17 External review comments incorporated
  - 10/20-11/03: 2nd external review period
  - 11/17: Incorporate comments from 2nd external review
  - 11/19-12/19: New draft presented for NIAC review
  - Mid-December: Final changes made based on NIAC review
  - Late December: NIAC-approved version delivered to DHS for final printing and preparation
- Formal presentation to the President in January 2004

Comments and Suggestions

- Principal authors:
  - Adam Rak, Symantec
  - Jim Duncan, Cisco Systems
- Additional contacts:
  - Rob Clyde, Symantec
  - Ken Watson, Cisco Systems
- Editors' e-mail address:
  - niac-vdwg@external.cisco.com